Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A data transfer apparatus for secure transfer~~,~~ from a digital data source to a digital data receiver~~,~~ of a plurality of data blocks each data block comprising plural frames of a digital video image, the apparatus comprising:

(a) an encryption key generator for providing encryption keys wherein a respective encryption key is assigned to each data block of the plurality of data blocks and a block synchronization index is provided indicating a correspondence between said encryption key and said data block, said block synchronization index is computed using a pseudo-random number generator;

(b) an encryption engine that, for each said data block, produces an encrypted data block using said encryption key from said encryption key generator;

(c) a data transmission channel for delivering said encrypted data block from said encryption engine to the digital data receiver;

(d) a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver;

(e) a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver;

(f) a memory for storing the encryption keys at the digital data receiver; and

(g) said digital data receiver including a decryption engine that is responsive to said synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block.

2. (previously presented) The apparatus of claim 1 wherein said encryption engine and decryption engine are provided with symmetric encryption.

3. (currently amended) The apparatus of claim 1 wherein the size of said ~~single~~ data block is further conditioned by an offset value.

4. (canceled)

5. (original) The apparatus of claim 1 wherein said data transmission channel is a wireless transmission network.

6. (original) The apparatus of claim 1 wherein said data transmission channel utilizes dedicated phone service.

7. (original) The apparatus of claim 1 wherein said data transmission channel utilizes a portable storage medium.

8. (original) The apparatus of claim 1 wherein said data transmission channel utilizes a computer data network.

9. (original) The apparatus of claim 1 wherein said data transmission channel utilizes a local area network.

10. (original) The apparatus of claim 1 wherein said data transmission channel utilizes a wide area network.

11. (previously presented) The apparatus of claim 1 wherein said block synchronization data channel utilizes a smart card.

12. (previously presented) The apparatus of claim 1 wherein said block synchronization index is encrypted.

13. (previously presented) The apparatus of claim 1 wherein said block synchronization data channel utilizes a portable storage medium.

14. (previously presented) The apparatus of claim 1 wherein said key transmission channel utilizes a smart card.

15. (previously presented) The apparatus of claim 1 wherein said encryption key is encrypted.

16. (previously presented) The apparatus of claim 1 wherein said key transmission channel utilizes a portable storage medium.

17. (original) The apparatus of claim 1 wherein said data block is compressed.

18. (canceled)

19. (currently amended) The apparatus of claim ~~18~~ 1 wherein said pseudo-random number generator is a linear feedback shift register.

20. (original) A method for secure transfer of a data stream from a digital data source to a digital data receiver, the method comprising:

(a) partitioning the data stream into a plurality of successive data blocks, wherein the size of each successive data block is variable, based on an average size and based on a randomly generated offset;

(b) generating, for each successive data block, an encryption key;

(c) encrypting each said successive data block using said encryption key to provide an encrypted data block; and

(d) generating a synchronization index associating said encrypted data block with said encryption key.

21. (original) The method of claim 20 wherein the step of providing said encrypted data block comprises the step of recording said encrypted data block onto a recording medium.

22. (original) The method of claim 21 wherein said recording medium uses a magnetic storage technology.

23. (original) The method of claim 21 wherein said recording medium uses an optical storage technology.

24. (original) The method of claim 20 wherein the step of providing said encrypted data block comprises the step of transmitting said encrypted data block to the digital data receiver.

25. (original) The method of claim 20 further comprising the step of encrypting said encryption key.

26. (original) The method of claim 20 further comprising the step of transmitting said encrypted data blocks to said receiver site in non-sequential order.

27. (original) The method of claim 20 wherein said data stream comprises digital motion image data.

Claims 28-35 (cancelled)

36. (currently amended) A method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion ~~the late that~~ image, the method comprising:

(a) providing said plurality of encryption keys separately from said encrypted data blocks and storing the encryption keys in a memory at a digital data receiver;

(b) providing an identifier that correlates a mapping algorithm to said plurality of encryption keys; ~~and~~

(c) operating a decryption engine that is responsive to said identifier and the mapping algorithm to generate each key for use in decryption of the respective data ~~block.~~ block;

wherein the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part; and

wherein a digital motion image data frame comprises plural color components and only data of one of the color components is encrypted.

37. (original) The method of claim 36 wherein said plurality of encryption keys are interleaved in a non-sequential order.

38. (original) The method of claim 36 further comprising the step of padding said plurality of encryption keys using dummy bits.

39. (cancelled)

40. (currently amended) The method of claim ~~39~~ 36 wherein each block is a digital motion image data frame component of a motion picture.

41. (currently amended) The method of claim ~~39~~ 36 wherein each block is a digital motion image data frame of a motion picture.

42. (currently amended) The method of claim ~~39~~ 36 wherein decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen.

43. (cancelled)

44. (currently amended) The method of claim ~~39~~ 36 wherein the digital motion image data blocks are compressed using an MPEG type of

compression to form intra-coded stand alone frames and dependent P and B frames, and the intra- coded and P and B frames are encrypted.

45. (cancelled)

46. (currently amended) The method of claim ~~45~~ 36wherein the color component that is encrypted is represented by a bit depth greater than one and only one bit plane of the color component data is encrypted.

47. (currently amended) A method of decrypting encrypted digital motion image data blocks of a motion picture comprising:

providing digital motion image data of a digital motion picture as digital motion image data blocks at least some of which digital motion image data blocks are of different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks; ~~and~~

in response to an index providing information identifying a first frame of each digital motion image data block generating a corresponding key from a plurality of encryption keys for use in decrypting a respective digital motion image data block wherein the said at least some digital motion image data blocks each represents plural frames of the motion ~~picture.~~ picture; and

wherein a digital motion image data frame comprises plural color components and the data of the color components are encrypted and further wherein each color component is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of each color component data is encrypted.

48. (canceled)

49. (canceled)

50. (original) The method of claim 47 wherein the decryption of the encrypted data blocks is made in a digital motion image projector which projects images represented by the digital motion image data upon a screen.

51. (canceled)

52. (canceled)

53. (previously presented) A method of decrypting encrypted digital motion image data blocks of a motion picture comprising:

providing digital motion image data of a digital motion picture as digital motion image data blocks, wherein a digital motion image data frame comprises plural color components and only data of one of the color components is encrypted; and

generating a corresponding key from a plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted.

54. (original) The method of claim 53 wherein the data of the color component that is encrypted is represented by a bit depth greater than one and one or more bit planes but less than all bit planes of the color component data is encrypted.

55. (cancelled)

56. (cancelled)

57. (previously presented) The method of claim 47 wherein block boundaries are determined by computation of random offsets.

58. (original) The method of claim 47 wherein indices providing correspondence information relative to encryption keys are provided in a channel separate from a channel providing ciphertext of the encrypted data blocks.

Claims 59-77 (canceled)